



Nick Feamster
Professor, Department of Computer Science
Acting Director, Center for Information
Technology Policy

310 Sherrerd Hall
Center for Information Technology Policy
Princeton University
Princeton, New Jersey 08540-5233
+1 609 258 2203
feamster@cs.princeton.edu

July 13, 2016

To Whom It May Concern:

On Friday, July 9, 2016, I presented to the FCC's Wireline Competition Bureau on the topic of ISPs and privacy. The contents of the presentation are attached.

The following people were in attendance: David Brody, Melissa Kinkel, Brad Bourne, Gail Grutov, Baraki Middleton, Sherwin Siy, Jonathan Mayer, Lisa Honc, Matt DelNero, Brian Hurley, and Scott Jordan.

The attached slides contain the topic of presentation, which was to illustrate the many varied datasets that ISPs have at their disposal to improve the performance and security of the network.—as well as the privacy concerns that each of these datasets might pose.

We discussed the need to exempt researchers from the FCC's rulemaking, as network research fundamentally depends on access to ISP data, ranging from NetFlow/IPFIX to DNS. We discussed both the sensitivities of these datasets, as well as how they are used in practice to ensure that the network is secure and performs well.

Discussion touched on many topics, including questions about specific circumstances where researchers would need access to either disaggregated (*i.e.*, individual) or non-anonymized traffic datasets. We discussed scenarios when researchers could make use of anonymized or aggregated data, as well as scenarios concerning network performance or security where traffic traces from individual devices would be necessary to design and evaluate the algorithm.

Two questions came up for follow-up discussion:

- Propose precise wording for the researcher exemption. The intent should be to protect academic researchers while minimizing the possibility for loopholes that could be construed as research but are not strictly academic research.
- Provide examples of cases where researchers have made use of anonymized but *disaggregated* network traffic data (*i.e.*, data from individual users), to make a case for exceptions to the need to aggregate network traffic data before releasing it to researchers.

I plan to file further comment on these questions.

Thank you for your consideration.

Sincerely,

A handwritten signature in black ink, appearing to be "Nick Feamster", written in a cursive style.

Nick Feamster